UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA

ANITA ROBERTSON HULSE, DARI VIZIER, DYLAN STANFORD, ANGELA BROUSSARD, APRIL BUTLER, BENJAMIN FONTENOT, PATRICA BROOKS, DWAYNE PITRE, and DONOVAN CORREA *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

ACADIAN AMBULANCE SERVICE, INC.

Defendant.

JURY DEMAND ENCLOSED

CASE NUMBER: 6:24-cv-01011-DCJ-CBW

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Anita Robertson Hulse, Dari Vizier, Dylan Stanford, Angela Broussard, April Butler, Benjamin Fontenot, Patricia Brooks, Dwayne Pitre, and Donovan Correa ("Plaintiffs") bring this Consolidated Amended Class Action Complaint against Defendant Acadian Ambulance Service, Inc. ("Acadian" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege as follows:

INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similarly situated current and former Defendant employees' and customers' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII") and protected health information ("PHI"), including names, dates of birth, Social Security numbers, medical record numbers, and medical and

treatment information (collectively, "PII and PHI" shall be referred to as the "Private Information") from cybercriminals.

2. Defendant Acadian, a private ambulance service business based in Lafayette, Louisiana, operates throughout Louisiana, Texas, Tennessee, and Mississippi. Defendant has stated that its fleet of 500 ambulances and med flight helicopters transport about 600,000 patients annually and travel 38 million miles each year.[1]

3. As a condition of receiving services from Defendant, Plaintiffs and Class Members were required to entrust Defendant with their sensitive Private Information including their names, dates of birth, Social Security numbers, medical records, case histories, physicians' notes, suspected drug use, laboratory test results, and other confidential personal information. Plaintiffs and Class Members provided their confidential information on the condition and with the understanding that Defendant would take reasonable measures to safeguard that information.

4. Defendant's failure to implement and maintain reasonable data security measures resulted in a well-known cybercriminal organization, called Daixin Team, accessing and exfiltrating Plaintiffs' and Class Members' Private Information, including full names, Social Security numbers, dates of birth, medical record numbers, and medical and treatment information (the "Data Breach") in June 2024.[2] As many as 2.9 million individuals had their Private Information disclosed.[3]

5. Daixin Team demanded that Defendant pay a ransom of $7,000,000 for the return of the Private Information exfiltrated in the Data Breach. Defendant refused to pay this ransom,

---

[1] *See* https://www.bankinfosecurity.com/acadian-ambulance-notifying-nearly-3-million-data-theft-a-26235 (last visited November 20, 2024).
[2] https://www.hipaajournal.com/acadian-ambulance-ransomware-attack/ (last visited November 20, 2024).
[3] *Id.*

instead offering to pay $173,000, which Daixin Team rejected.[4] As a result, Plaintiffs' and Class Members' Private Information is at continued and heightened risk of being leaked on the dark web.

6. In fact, Daixin Team has already claimed to have published Plaintiffs' and Class Members' Private Information "including records involving patient case histories, 'suspected drug use,' and physician 'care point' documentation. The leak site used by Daixin Team also lists files allegedly pertaining to Acadian employees."[5]

7. Despite the now certain fact that Private Information stolen in the Data Breach will be used maliciously by fraudsters and identity thieves, Defendant did not start notifying victims of the Data Breach, including Plaintiffs, until July 2024—long after recognizing the risk that Plaintiffs and Class Members were facing.

8. Although Defendant has reprehensibly chosen to keep many details of the Data Breach secret, the evidence available thus far indicates that it is more likely than not that Defendant failed to implement and maintain reasonable data security measures. For example, Defendant did not properly encrypt or redact Private Information, retained Private Information longer than necessary, and failed to adequately secure user credentials for internet-facing applications on its network. Defendant also failed to limit access to Private Information stored on an internet accessible environment to only necessary individuals and failed limit access to multi-factor authenticated individuals. Defendant further failed to implement adequate network monitoring and protocols for detecting unauthorized intrusions. Had it done so it may have prevented or mitigated the exfiltration of unencrypted data from its systems.

[4] *Id.*
[5] *Supra* n. 1.

PARTIES

Plaintiffs

9. Plaintiff Anita Robertson Hulse is an adult individual and a natural person of Texas, residing in Bell County, where she intends to stay.

10. Plaintiff Hulse provided her information to Acadian in the course of obtaining services from Acadian in or about 2023.

11. Plaintiff Hulse learned of the Data Breach in or about July 2024 when she was informed of the Data Breach.

12. Plaintiff Dari Vizier is an adult individual and a natural person of Louisiana, residing in Lafourche Parish, where she intends to stay.

13. Plaintiff Vizier provided her information to Acadian in the course of receiving emergency medical services in 2022.

14. Plaintiff Vizier first learned of the Data Breach on or about July 2024 when a friend informed her of the Data Breach and the potential exposure of her Private Information.

15. Plaintiff Dylan Stanford is an adult individual and a natural person of Louisiana, residing in Beauregard Parish County, where he intends to stay.

16. Plaintiff Stanford provided his information to Acadian in the course of his employment with Defendant from approximately 2020 through 2022.

17. Plaintiff Stanford learned of the Data Breach on or about July 2024 when he saw something online regarding the data breach, including that it had included employee information, informing him of the Data Breach and the exposure of his Private Information.

18. Plaintiff Angela Broussard is an adult individual and a natural person of Louisiana, residing in Terrebone Parish, County, where she intends to stay.

19. Plaintiff Broussard provided her information to Acadian in the course of an auto accident and Acadian responded to the call.

20. Plaintiff Angela Broussard learned of the Data Breach on or about April of 2024 when she saw it on online informing her of the Data Breach and the exposure of her Private Information.

21. Plaintiff Benjamin Fontenot is an adult individual and a natural person of Louisiana residing in Saint Landry Parish, where he intends to stay.

22. Plaintiff Fontenot provided his information to Acadian both as a condition of employment and in the course of receiving services from Acadian.

23. Plaintiff Fontenot learned of the Data Breach on or about August 2024 through a friend informing him of the Data Breach and the exposure of his Private Information.

24. Plaintiff April Butler is an adult individual and a natural person in the State of Texas, residing in Orange County, where she intends to stay.

25. Plaintiff Butler provided her information to Acadian in the course of using its ambulance services, including in March of 2024.

26. Plaintiff Butler learned of the Data Breach when she saw something online regarding the Data Breach specifically referencing the Defendant.

27. Plaintiff Patricia Brooks is an adult individual and a natural person of Louisiana residing in Covington, Louisiana, where she intends to stay.

28. Plaintiff Brooks provided her information to Acadian in the course of receiving ambulatory services from Acadian.

29. Plaintiff Brooks learned of the Data Breach on or about August 2024 when she discovered various internet sources reporting on the Data Breach.

30. Plaintiff Dwayne Pitre is an adult individual and a natural person of Louisiana, residing in St. Landry Parish, where he intends to stay.

31. Plaintiff Pitre provided his information to Acadian as a condition of receiving ambulance services.

32. Plaintiff Pitre learned of the Data Breach in June 2024 in the news media.

33. Plaintiff Donovan Correa is an adult individual and a natural person of Texas, residing in Bastrop County, where he intends to stay.

34. Plaintiff Correa provided his information to Acadian in the course of his employment as a medic with Acadian.

35. Plaintiff Correa learned of the Data Breach on or around June 26, 2024, when he received an internal email from Acadian's leadership regarding a network security incident, informing him of the Data Breach and the exposure of his Private Information.

Defendant Acadian Ambulance Service

36. Defendant is a private ambulance service business incorporated in the State of Louisiana and headquartered at 130 E. Kaliste Saloom Road, Lafayette, LA 70508.

JURISDICTION AND VENUE

37. This Court has original subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). First, because the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs. Second, because this class action involves a putative class of over 100 members. And third, because there is sufficient diversity—while Defendant's principal place of business is in Louisiana, many Class Members are citizens of different states.

38. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in Louisiana, and Defendant regularly conducts business in Louisiana, and has a location in New Orleans, Louisiana.

39. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, Defendant conducts substantial business in this District, and Defendant is headquartered in Lafayette, Louisiana.

FACTUAL ALLEGATIONS

Background

40. Plaintiffs and the Class Members, as current or former employees and customers, reasonably relied (directly or indirectly) on this large medical services business to keep their sensitive Private Information confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their Private Information. People, including Plaintiffs, demand security to safeguard their Private Information, especially when Social Security numbers and sensitive health information are involved as here.

41. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiffs, Defendant promised to provide confidentiality and adequate security from the data it collected from patients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

42. Defendant states on its website that: "Our vision is for the name "Acadian" to be synonymous with the best health, safety and security services in the nation and the world."[6]

[6] *See* https://acadianambulance.com/our-company/company-culture/ (last visited November 20, 2024).

43. Due to the highly sensitive and confidential nature of the information Defendant acquires and stores with respect to its patients, Defendant is required to keep patients' Private Information private; comply with industry standards related to data security and the maintenance of their patients' Private Information; inform their patients of its legal duties relating to data security; comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services they provide; and provide adequate notice to patients if their Private Information is disclosed without authorization.

44. Defendant's Notice of Practices states, "We are required by law to maintain the privacy and security of your protected health information. We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[7]

45. Without the required submission of Private Information from Plaintiffs and Class Members, Defendant could not perform the services it provides.

46. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

47. Defendant's actions and inactions directly resulted in the Data Breach and the compromise of Plaintiffs' and Class Members' Private Information.

48. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties and as evidenced by the Data Breach, it failed to adhere to that duty.

[7] *See* https://web.archive.org/web/20240827151353/https://acadian.com/wp-content/uploads/Noticy-of-Privacy-Practices.pdf/ (last visited November 20, 2024).

The Data Breach

49. On or around June 2024, Daixin Team executed a targeted and foreseeable attack of Defendant's computer network that allowed it to steal the highly sensitive PII and PHI of Plaintiffs and Class Members. According to Daixin Team, it made off with approximately the records of 11 million customers and employees.[8] Defendant states the Data Breach involved "the protected health information of 2,896,985 individuals."[9]

50. Publicly available articles covering the breach have confirmed that impacted Private Information included full names and Social Security numbers, dates of birth, medical record numbers, and medical treatment information.[10]

The Data Breach was Foreseeable.

51. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

52. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[8] *See* https://www.cpomagazine.com/cyber-security/acadian-ambulance-services-leaks-protected-health-information-after-cyber-attack/ (last visited November 20, 2024).

[9] *See* https://www.hipaajournal.com/acadian-ambulance-ransomware-attack/; *see also* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (wherein Defendant reported to the U.S. Government that 2,896,985 individuals were affected.). (last visited November 20, 2024).

[10] *Supra* n. 7.

53. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[11]

54. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.[12] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[13] Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.[14] In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[15]

55. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[16] As cybersecurity

---

[11] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited November 20, 2024).

[12] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

[13] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

[14] *Ponemon study finds link between ransomware, increased mortality rate*, available at https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate

[15] *The State of Ransomware in Healthcare 2022*, available at https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf

[16] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

56. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[17] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[18] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[19] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[20]

57. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

58. In 2021, a record 1,862 data breaches occurred, with 330 of them, or 17.7%, in the medical or healthcare industry.[21] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[22]

---

[17] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[18] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[19] *Id.*

[20] *Id.*

[21] *See* 2021 Data Breach Annual Report, 6 (ITRC, Jan. 2022) available at https://notified.idtheftcenter.org/s/ (last visited November 20, 2024).

[22] *Id.*

59. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issued a warning to potential targets in 2019, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[23]

60. Entities in custody of PHI, like Defendant, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[24]

61. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[25] Almost fifty percent of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy.[26]

---

[23] FBI, Secret Service Warn of Targeted, Law360 (Nov.18, 2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware (last visited November 20, 2024).

[24] *See* Identity Theft Resource Center, 2022 Annual Data Breach Report, ITRC (Jan. 2023) https://www.idtheftcenter.org/publication/2022-data-breach-report (last visited November 20, 2024).

[25] *See* Elinor Mills, Study: Medical identity theft is costly for victims, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited November 20, 2024).

[26] *Id.*

62. A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for about $1.22 According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[27]

63. As a major healthcare provider, Defendant knew, or should have known, the importance of safeguarding the patients' Private Information entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Defendant's patients because of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

The Data Breach was a Specifically Foreseeable Risk of which Defendant was on Notice

64. It is well known that Private Information, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

[27] Brian O'Connor, Healthcare Data Breach: What to Know About them and What to Do After One, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited November 20, 2024).

65. At the time of the Data Breach, even more specifically, the threat posed by Daixin Team was known, or should have been known, by Defendant. Experts have described Daixin Team as "a cybercrime group that is actively targeting U.S. businesses, predominantly in the Healthcare and Public Health (HPH) Sector, with ransomware and data extortion operations.[28]

66. At the time, Daixin Team has committed other such well documented techniques to target providers like Defendant. As one publication noted in a report about the Data Breach, "Daixin Team cybercrime actors have caused ransomware incidents at multiple HPH Sector organizations[.]"[29]

67. On October 21, 2022, the FBI and CISA released a joint advisory (the "Joint Advisory") detailing the risk posed by Daixin Team to Healthcare and Public Health Sector providers, the common techniques employed by Daixin Team, and mitigation measures known to prevent Daixin Team attacks.[30]

Defendant Failed to Implement & Maintain Reasonable Security

68. As discussed above, the Joint Advisory details the specific methods of attack used by Daixin Team, along with how to prevent them.

69. Specifically, "Daixin actors gain initial access to victims through virtual private network (VPN) services."[31]

70. Given that Daixin Team likely effectuated the Data Breach through compromised computer systems, it is more likely than not that the "bad practices" identified by CISA were employed by Defendant at the time of the Data Breach.

---

[28] https://www.cisa.gov/sites/default/files/2023-07/aa22-294a-stopransomware-daixin-team.pdf (last visited November 20, 2024).
[29] *Id.*
[30] *See Id.*
[31] *Id.*

71. The access to and exfiltration of PII and PHI by Daixin Team would not have occurred but for Defendant's failure to implement and maintain the data security measures discussed in the Joint Advisory and other advisory materials.

72. Regardless of Defendant's failure to properly secure and monitor Private Information, Defendant was also grossly negligent in its decision to not properly encrypt or redact the Personal Information in its possession, as well as its decision to hold Private Information for longer than it had a legitimate use. For example, Plaintiff Fontenot has not been affiliated with Defendant for two years. Yet, Defendant inexplicably decided to continue storing Plaintiffs' and Class Members' Private Information on its systems long after their affiliation with Defendant ended.

73. Several best practices have been identified for entities like Defendant that store PII and PHI, including but not limited to educating all employees; using strong passwords; implementing multi-layer security measures such as firewalls, anti-virus, and anti-malware software; encrypting data to make it unreadable without a key; employing multi-factor authentication; backing up data; and limiting employee access to sensitive information.

74. Other best cybersecurity practices that are standard in the data security industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

75. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02,

PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

77. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because Defendant failed to properly maintain and safeguard their computer systems and network. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect PII and PHI;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PII and PHI it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII and PHI to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII and PHI;

j. Failing to train all members of their workforces effectively on the policies and procedures regarding PII and PHI;

k. Failing to render the electronic PII and PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, 15 U.S.C. § 45;

m. Failing to adhere to industry standards for cybersecurity as discussed above; and,

n. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII and PHI.

78. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII and PHI by allowing cyberthieves to access Defendant's inadequately secured network, which provided unauthorized threat actors with unsecured and unencrypted PII and PHI.

79. Consequently, as detailed below, Plaintiffs and Class Members now face an immediate, heightened risk of fraud and identity theft. Additionally, Plaintiffs and the Class Members lost the benefit of the bargain they made with Defendant.

The Theft of PII and PHI Has Severe & Long-Lasting Consequences

80. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII and PHI secure are long lasting and severe. Once PII and PHI are stolen, particularly Social

Security numbers as here, fraudulent use of that information and damage to victims is likely to continue for years.

81. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

82. This is because any victim of a data breach is exposed to severe consequences regardless of the nature of the data. In fact, criminals steal personally identifiable information to monetize it by selling the stolen data on the black market to identity thieves who aim to extort and harass victims or take over their identities to engage in illegal financial transactions under the victims' names.

83. Social Security numbers are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

84. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social

[32] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited November 20, 2024).

Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

85. By failing to properly notify Plaintiffs and the Class Members of the Data Breach, Defendant exacerbated their injuries. Specifically, by depriving them of the chance to take speedy measures to protect themselves and mitigate harm, Defendant allowed their injuries to fester and the damage to spread.

86. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[33]

87. In addition to opening new bank or payment card accounts, attackers can use an individual's Social Security number, in combination with information like names, addresses, dates of birth, and/or phone numbers, to bypass account security protocols and access an individual's existing bank and payment card accounts.[34]

---

[33] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited November 20, 2024).

[34] *See* https://reasonlabs.com/blog/7-things-hackers-can-do-with-your-stolen-social-security-number-and-6-ways-to-protect-it (last visited November 20, 2024);

88. Trying to change or cancel a stolen Social Security number is incredibly difficult, if not impossible. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

89. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

90. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[36]

91. It can take years for victims to notice their identity was stolen—giving criminals plenty of time to sell one's personal information to the highest bidder.

92. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security

---

https://www.moneytalksnews.com/slideshows/heres-what-hackers-can-do-with-your-social-security-number/ (last visited November 20, 2024).

[35] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited November 20, 2024).

[36] *See* https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf (last visited November 20, 2024).

number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

93. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

94. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[37]

95. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

96. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other

[37] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm,* Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited on November 20, 2024).

words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

97. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

98. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

99. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[38] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[39] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

[38] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited November 20, 2024).
[39] *Id* at 4.

100. As demonstrated by the repeated attempts at identity theft and fraud that Plaintiffs have suffered, that is exactly what is happening to Plaintiffs and Class Members. And it is reasonable for any trier of fact, including this Court or a jury, to find that the stolen PII and PHI (of Plaintiffs and the other Class Members) is being misused—and that such misuse is fairly traceable to Defendant's data breach.

101. Responsible for handling highly sensitive personal information, Defendant knew or should have known the importance of safeguarding PII and PHI. Defendant also knew or should have known of the foreseeable consequences of a data breach. These consequences include the significant costs imposed on victims of the breach. Still, Defendant failed to take adequate measures to prevent the data breach.

102. Due to Defendant's inadequate practices, the PII and PHI of Plaintiffs and Class Members were exposed to criminals. In other words, Defendant disclosed and exposed its PII and PHI to malicious operators and criminals. These criminals engage in disruptive and unlawful activities such as online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud)—all using stolen Private Information.

103. Given the nature of Defendant's Data Breach it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain Plaintiffs' and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

104. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, simple credit card information in a

retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[40] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

105. To date, Defendant has not offered Plaintiffs and Class Members *any* sort of recovery or protective service in response to the Data Breach. This is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly considering the Private Information at issue here.

106. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures to protect PII and PHI that it maintained.

The Value of Private Information

107. Stolen personal information is one of the most valuable commodities on the information black market. According to Experian, a credit-monitoring service, stolen personal information can sell for over $1,000.00 (depending on the type of information).[41]

108. Private Information like the Social Security numbers stolen in this case demand a premium on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[42]

---

[40] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited November 20, 2024).

[41] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited November 20, 2024).

[42] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015),

109. The value of Plaintiffs' and Class Members' Private Information on the black market is considerable. Stolen personal information trades on the black market for years, and criminals frequently post stolen Private Information openly and directly on various "dark web" internet websites. Thus, after charging a substantial fee, criminals make such stolen information publicly available.

110. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[43] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[44]

111. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is likely readily available to others, and the rarity of the PII has been destroyed, thereby causing additional loss of value.

Defendant Failed to Comply with FTC Guidelines

112. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for

---

https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited November 20, 2024).

[43] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited November 20, 2024).

[44] *See* https://datacoup.com/ (last visited November 20, 2024).

business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[45]

113. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[46] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[47]

114. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[48] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

115. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[49]

116. The FTC recommends that businesses:

---

[45]Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited November 20, 2024)

[46] 17 C.F.R. § 248.201 (2013).

[47] *Id*.

[48]Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited November 20, 2024).

[49] FTC, *Start with Security*, *supra* note 59.

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection

a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

117. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

118. Since Class Members entrusted Defendant with their Private Information, either directly or indirectly, Defendant had, and continues to have, a duty to keep their Private Information secure.

119. Plaintiffs and the other Class Members reasonably expected that when they provide Private Information to Defendant that such Private Information would be protected and safeguarded.

120. Defendant was at all times fully aware of its obligation to protect the Private Information of its customers and current and former employees, including Plaintiffs and Class Members. Defendant was also aware of the significant repercussions if it failed to do so.

121. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiffs' and Class Members' Private Information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Failed to Comply with HIPAA Requirements

122. Defendant is required by HIPAA to safeguard patient PHI.

123. Defendant is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

124. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

125. Further to 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

126. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an

individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

127. HIPAA requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq.*

128. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

129. Given the application of HIPAA to Defendant, and that Plaintiffs and Class Members entrusted their PHI to Defendant in order to receive healthcare services, Plaintiffs and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

130. In addition to failing to follow universal data security practices, Defendant failed to follow healthcare industry standard security practices, including:

a. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

b. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

c. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

d. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c).

131. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[50] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

132. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

133. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[51]

[50] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.
[51] Breach Notification Rule, U.S. Dep't of Health & Human Services,

Plaintiffs and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach It Allowed

134. Plaintiffs and Class Members reasonably expected Defendant to provide adequate security protections for their PII and PHI, and therefore, entrusted Defendant with sensitive personal information, including their Social Security numbers.

135. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to work for Defendant or utilize Defendant's services as a customer, Plaintiffs and other Class Members reasonably understood and expected that their Private Information would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

136. Cybercriminals target and capture Private Information to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

137. The cybercriminals who targeted and obtained Plaintiffs' and Class Members' PII and PHI may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other Private Information, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;

---

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited November 20, 2024).

- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

138. Additionally, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, which can impair their ability to gain employment or obtain a loan.

139. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their Private Information, for which there is a well-established national and international market.

140. Furthermore, certain Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[52]

141. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[53] Indeed, "[t]he level of risk is growing for

[52] *Id.*

[53] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (Feb. 23, 2012), https://web.archive.org/web/20170228020506/http://www.iii.org/insuranceindustryblog/?m=201202 (last visited November 20, 2024).

anyone whose information is stolen in a data breach."[54] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[55] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' Private Information will do so at a later date or re-sell it.

142. As a result of the Data Breach, Plaintiffs and Class Members have already suffered damages and will continue to suffer damages.

Plaintiff Anita Robertson Hulse's Experience

143. Plaintiff Anita Robertson Hulse is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Hulse stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Hulse diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be.

144. Plaintiff Hulse is similarly cautious in the use and disclosure of her PHI, including information about her medications, appointments, diagnoses, and any treatments she has been prescribed by any medical practitioners.

---

[54] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), https://web.archive.org/web/20200311212052/http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last visited November 20, 2024).

[55] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://web.archive.org/web/20220131125035if_/https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last visited November 20, 2024).

145. Plaintiff Hulse only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. Upon information and belief, Plaintiff Hulse's Private Information was within the possession and control of Defendant at the time of the Data Breach.

146. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Hulse suffered injury from a loss of privacy.

147. Plaintiff Hulse has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Hulse entrusted to Defendant. This information has inherent value that Plaintiff Hulse was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

148. Upon information and belief, Plaintiff Hulse's Personal Information has already been stolen and misused.

149. The Data Breach has also caused Plaintiff Hulse to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

150. As a result of the actual harm she has suffered and the increased imminent risk of future harm.

151. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Hulse to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring her

accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

152. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Hulse to suffer stress, fear, and anxiety.

153. Plaintiff Hulse has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Dari Vizier's Experience

154. Plaintiff Dari Vizier is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Vizier stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Vizier diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff Vizier uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

155. Plaintiff Vizier is similarly cautious in the use and disclosure of her PHI, including information about her medications, appointments, diagnoses, and any treatments she has been prescribed by any medical practitioners.

156. Plaintiff Vizier only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access

databases storing her Private Information. As a result, Plaintiff Vizier's Private Information was within the possession and control of Defendant at the time of the Data Breach.

157. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Vizier suffered injury from a loss of privacy.

158. Plaintiff Vizier has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Vizier entrusted to Defendant. This information has inherent value that Plaintiff Vizier was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

159. Upon information and belief, Plaintiff Vizier's Personal Information has already been stolen and misused as a ransomware gang Daixin clams to have published the Data Breach victims' data on its dark web leak site.

160. Furthermore, Plaintiff Vizier has experienced increased spam emails and texts as a result of the Data Breach.

161. The Data Breach has also caused Plaintiff Vizier to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

162. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Vizier spent time putting a credit freeze on her accounts, as well as reviewing and forwarding spam emails and texts to her attorneys.

163. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Vizier to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring her

accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

164. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Vizier to suffer stress, fear, and anxiety, including fear of identity theft, medical fraud, and anxiety concerning her medical history and the details of medical services she received from Acadian being made public.

165. Plaintiff Vizier has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Dylan Stanford's Experience

166. Plaintiff Dylan Stanford is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Stanford stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Stanford diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff Stanford uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

167. Plaintiff Stanford only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Stanford's Private Information was within the possession and control of Defendant at the time of the Data Breach.

168. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Stanford suffered injury from a loss of privacy.

169. Plaintiff Stanford has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Stanford entrusted to Defendant. This information has inherent value that Plaintiff Stanford was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

170. Upon information and belief, Plaintiff Stanford's Personal Information has already been stolen and misused as he has experienced a substantial uptick in the amount of spam that he has been receiving on his phone and email account previously affiliated with his employment. Many of these spam attempts have used pieces of the compromised PII in phishing attempts designed to get Plaintiff Stanford to disclose even more of his Private Information. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Stanford's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

171. The Data Breach has also caused Plaintiff Stanford to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

172. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Stanford has spent more than five hours so far on activities directly related to this Data Breach, including researching the legitimacy of the Data Breach, researching ways to protect himself, changing passwords and account credentials, and reviewing his bank accounts and credit reports for fraud. He has also been forced to spend time fielding all of the spam he has been receiving.

173. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Stanford to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

174. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Stanford to suffer stress, fear, and anxiety that is typical and expected for someone who now faces such a dramatically increased risk of identity theft and fraud for years to come.

175. Plaintiff Stanford has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Angela Broussard's Experience

176. Plaintiff Angela Broussard is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Broussard stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Broussard diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff Broussard uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

177. Plaintiff Broussard is similarly cautious in the use and disclosure of her PHI, including information about her medications, appointments, diagnoses, and any treatments she has been prescribed by any medical practitioners.

178. Plaintiff Broussard only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Broussard's Private Information was within the possession and control of Defendant at the time of the Data Breach.

179. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

180. Plaintiff Broussard has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Broussard entrusted to Defendant. This information has inherent value that Plaintiff Broussard was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

181. Upon information and belief, Plaintiff Broussard's Personal Information has already been stolen and misused as she experienced an increase of spam calls and texts. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Broussard's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

182. Furthermore, Plaintiff Broussard has experienced an increase of spam calls and texts as a result of the Data Breach.

183. The Data Breach has also caused Plaintiff Broussard to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

184. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Broussard has lost time monitoring her accounts.

185. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Broussard to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

186. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Broussard to suffer stress, fear, and anxiety.

187. Plaintiff Broussard has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff April Butler's Experience

188. Plaintiff Butler is a cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Butler stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Butler diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Butler uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

189. Plaintiff Butler is similarly cautious in the use and disclosure of her PHI, including information about her surgeries, conditions, medications, appointments, diagnoses, and any treatments she has been prescribed by any medical practitioners.

190. Ms. Butler only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information, and because she did not think she had a choice otherwise since it is the only ambulance service in her area. As a result, Plaintiff Butler's Private Information was within the possession and control of Defendant at the time of the Data Breach.

191. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Butler suffered injury from a loss of privacy.

192. Plaintiff Butler has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Butler entrusted to Defendant. This information has inherent value that Plaintiff Butler was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

193. Upon information and belief, Plaintiff Butler's Personal Information has already been stolen and misused as a result of the Data Breach. She has experienced specific, targeted incidents of fraud and identity theft, including medical insurance identity theft and tax-related identity theft. Specifically, someone (in Florida) obtained health insurance from the "marketplace" using her information, including her Social Security Number, and maintained the coverage for a full year. It was only when that person went to renew coverage did it get flagged as fraud. Further, someone (in Houston) filed tax documents using her information as well. It is unknown what information that person had of hers, but it required significant remedial efforts by her, her tax consultant, and the IRS.

194. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Butler's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

195. Furthermore, in the aftermath of the Data Breach, Plaintiff Butler has suffered from a spike in spam emails and calls related specifically to health insurance issues as a result of the fraudulent activities on the health care marketplace. Upon information and belief, these are the result of the Data Breach.

196. The Data Breach has also caused Plaintiff Butler to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

197. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Butler has spent dozens of hours, mostly on the phone and online, with the IRS, her health insurance company, and her account, to remedy these issues.

198. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Butler to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring and remedying her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

199. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Butler to suffer stress, fear, and anxiety, in particular because Plaintiff Butler suffers from significant health issues and her PHI is incredibly important to her on a daily basis.

200. Plaintiff Butler has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected,

and safeguarded from future breaches. She would not have provided her Private Information if she had known about Defendant's lax data security protocols.

Plaintiff Benjamin Fontenot's Experience

201. Plaintiff Fontenot is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Fontenot stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Fontenot diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff Fontenot uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

202. Plaintiff Fontenot is similarly cautious in the use and disclosure of his PHI, including information about his medications, appointments, diagnoses, and any treatments he has been prescribed by any medical practitioners.

203. Plaintiff Fontenot only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Fontenot's Private Information was within the possession and control of Defendant at the time of the Data Breach.

204. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Fontenot suffered injury from a loss of privacy.

205. Plaintiff Fontenot has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Fontenot entrusted

to Defendant. This information has inherent value that Plaintiff Fontenot was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

206. Upon information and belief, Plaintiff Fontenot's Personal Information has already been stolen and misused as he has experienced a dramatic increase in suspicious spam telephone calls and text messages using his compromised Personal Information as a result of the Data Breach.

207. The Data Breach has also caused Plaintiff Fontenot to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

208. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Fontenot has spent approximately one hour every day since learning of the data breach monitoring his financial accounts and credit.

209. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Fontenot to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

210. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Fontenot to suffer stress, fear, and anxiety.

211. Plaintiff Fontenot has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Patricia Brooks' Experience

212. Plaintiff Brooks is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Brooks stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Brooks diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Brooks uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

213. Plaintiff Brooks is similarly cautious in the use and disclosure of her PHI, including information about her medications, appointments, diagnoses, and any treatments she has been prescribed by any medical practitioners.

214. Plaintiff Brooks only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Brooks's Private Information was within the possession and control of Defendant at the time of the Data Breach.

215. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Brooks suffered injury from a loss of privacy.

216. Plaintiff Brooks has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Brooks entrusted to Defendant. This information has inherent value that Plaintiff Brooks was deprived of when her

Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

217. In June of 2024, Plaintiff Brooks received an email and account notice from her bank informing her that its fraud detection service had discovered that her Private Information was available on the dark web. On information and belief, the Private Information unauthorized third parties have made available for purchase on the dark web was exfiltrated from Defendant during the Data Breach.

218. The Data Breach has also caused Plaintiff Brooks to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

219. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Brooks has spent approximately twenty minutes every day since learning of the data breach monitoring her financial accounts and credit.

220. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Brooks to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

221. As a result of the Data Breach, Plaintiff Brooks has incurred significant out-of-pocket expenses, including those incurred making three trips to her local bank to discuss the Data Breach with her personal banker.

222. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Brooks to suffer stress, fear, and anxiety.

223. Plaintiff Brooks has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Dwayne Pitre's Experience

224. Plaintiff Dwayne Pitre is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Pitre stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Pitre diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

225. Plaintiff Pitre is similarly cautious in the use and disclosure of his PHI, including information about his medications, appointments, diagnoses, and any treatments he has been prescribed by any medical practitioners.

226. Plaintiff Pitre only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Pitre's Private Information was within the possession and control of Defendant at the time of the Data Breach.

227. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Pitre suffered injury from a loss of privacy.

228. Plaintiff Pitre has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Pitre entrusted to

Defendant. This information has inherent value that Plaintiff Pitre was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

229. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Pitre's life as a whole, and specifically caused financial strain as a direct result of the Data Breach. For example, when the fraud occurred, it caused Mr. Pitre's bank account to be shut down while he was traveling for more than two months and thus unable to immediately visit his bank until he returned.

230. Furthermore, Plaintiff Pitre has experienced a significant increase in spam calls since the Data Breach and as a result of the Data Breach—often to the tune of about twenty to thirty per day.

231. The Data Breach has also caused Plaintiff Pitre to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

232. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Pitre to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring his accounts and credit report, visiting his bank (twenty minutes away) to close his bank account and open a new one, changing direct deposit information, and working with law enforcement to attempt to file a police report, among other tasks. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

233. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Pitre to suffer stress, fear, and anxiety because he has already begun seeing the effects and time

requirements associated with identity theft and financial fraud and worries about having to deal with the increased risk of such harm in the future.

234. Plaintiff Pitre has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Donovan Correa's Experience

235. Plaintiff Donovan Correa is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Correa stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Correa diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff Correa uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

236. Plaintiff Correa is similarly cautious in the use and disclosure of his PHI, including information about his date of birth, email address, physical address, telephone number, Social Security number, medical information, and other information he provided to Defendants upon employment with Acadian in 2023.

237. Plaintiff Correa only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Correa's Private Information was within the possession and control of Defendant at the time of the Data Breach.

238. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Correa suffered injury from a loss of privacy.

239. Plaintiff Correa has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Correa entrusted to Defendant. This information has inherent value that Plaintiff Correa was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

240. Upon information and belief, Plaintiff Correa's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of an unauthorized charge of five hundred dollars ($500) on his debit card and receiving alerts that his Private Information, such as his social security number, were found on the dark web. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Correa's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach. Plaintiff Correa suffered injury from the lost time value of his money while it was unavailable to him as a result of the fraud.

241. Furthermore, Plaintiff Correa has incurred late fees as a result of failed automatic payments associated with compromised bank accounts and has additionally experienced an increase of spam calls as a result of the Data Breach.

242. The Data Breach has also caused Plaintiff Correa to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

243. As a result of the actual harm, he has suffered and the increased imminent risk of future harm, Plaintiff Correa spent time signing up for a credit monitoring service, reviewing

accounts closely, resetting automatic billing instructions, and responding to a $500 fraudulent charge made on his debit card by contacting his bank and replacing his debit card.

244. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Correa to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

245. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Correa to suffer stress, fear, and anxiety as Plaintiff Correa is concerned of potential identity theft as a consequence of the data breach.

246. Plaintiff Correa has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CLASS ALLEGATIONS

247. Plaintiffs bring this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

248. Plaintiffs propose the following Nationwide Class definition, subject to amendments as appropriate.

> **All persons residing in the United States who were employed by or customers of Defendant whose PII and PHI may have been compromised in the Data Breach, including all those who were sent Notice.**

249. Plaintiffs Dari Vizier, Dylan Stanford, Angela Broussard, Benjamin Fontenot, Patricia Brooks, and Dwayne Pitre ("Louisiana Plaintiffs") also seek to represent a Louisiana Subclass of persons to be defined as follows:

> **All individuals residing in the State of Louisiana whose PII and/or PHI was compromised in the Defendant's Data Breach, including all those who were sent Notice (the "Louisiana Class").**

250. Excluded from the Classes are the following individuals and/or entities: Acadian Ambulance Service, and Acadian's parents, subsidiaries, affiliates, officers and directors, and any entity in which Acadian has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

251. Plaintiffs reserve the right to modify or amend the definition of the proposed classes and any future subclasses before the Court determines whether certification is appropriate.

252. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Classes consist of more than 10,000,000 individuals whose sensitive data was compromised in Data Breach.

253. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII and PHI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII and PHI;

f. Whether Defendant breached its duty to Class Members to safeguard their PII and PHI;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

254. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

255. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

256. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

257. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

258. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

259. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

260. The litigation of the claims presented here is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the identifiable Class Members demonstrate that prosecuting this lawsuit as a class action would not present significant manageability problems.

261. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

262. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, the Private Information

Defendant continues to maintain will remain at risk of future breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

263. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief regarding the Class Members as a whole is appropriate.

264. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' PII and PHI; and/or

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and All Class Members)

265. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

266. Defendant owed Plaintiffs and Class Members a duty to (1) implement and maintain reasonable security procedures appropriate to the nature of the information to protect PII and PHI from unauthorized access, destruction, use, modification, or disclosure; (2) take all reasonable steps to destroy records containing personal information that is no longer to be retained; and (3) notify individuals whose information may have been compromised in a data breach in the most expedient time possible and without unreasonable delay, but not later than sixty days from discovery of the breach. La. Rev. Stat. Ann. §§ 3074(A)-(E).

267. Defendant also had a duty arising under the FTC Act, the Louisiana Unfair Trade Practices Act, and HIPAA to employ reasonable measures to protect and secure PII and PHI, including by maintaining and testing security systems to ensure PII and PHI is adequately protected, implementing processes to timely detect security breaches, and complying with industry

security standards. 15 USC § 45(a)(1); La. Rev. Stat Ann. §§ 51:3074(A) & (J); 45 C.F.R. § 164.530(c)(l).

268. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance with industry standards concerning data security would result in the compromise of that PII and PHI — just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

269. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable classes of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and Class Members' PII and PHI.

270. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiffs and Class Members—which actually and proximately caused the Data Breach and injured Plaintiffs and Class Members.

271. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

272. Defendant's breach of its duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and All Class Members)

273. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

274. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

275. Moreover, Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

276. Defendant breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

277. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

278. Plaintiffs and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiffs and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

279. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

280. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that by failing to meet its duties, Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

281. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

282. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

283. Plaintiffs' and Class Members' PII and PHI was provided to Defendant as part of education services or employment that Defendant provided to Plaintiffs and Class Members.

284. Plaintiffs and Class Members agreed to be employed by Defendant or to pay for Defendant's ambulance services and provided their PII and PHI in the course of that relationship.

285. Defendant and Plaintiffs and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiffs' and Class Members' PII and PHI, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' PII and PHI.

286. Defendant had an implied duty of good faith to ensure that the PII and PHI of Plaintiffs and Class Members in its possession was only used in accordance with its contractual obligations.

287. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and PHI and to comply with industry standards and applicable laws and regulations for the security of this information.

288. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII and PHI, resulting in the Data Breach.

289. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in the breach of these contracts.

290. As a result of Defendant's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain.

291. Had Defendant disclosed that its data security was inadequate, neither Plaintiffs or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

292. As a result of Data Breach, Plaintiffs and Class Members suffered actual damages resulting from the theft of their PII and PHI, as well as the loss of control of their PII and PHI and remain at present risk of suffering additional damages.

293. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

294. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs. Plaintiffs bring this claim in the alternative to his breach of implied contract claim.

295. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have had their Private Information protected with adequate data security.

296. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form of their Private Information. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

297. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and some Class Members.

298. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

299. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

300. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

301. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

302. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

303. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

304. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, because

Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

305. Plaintiffs and Class Members have no adequate remedy at law.

306. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

307. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

308. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

309. Accordingly, Plaintiffs and Class members respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant

should have spent to provide reasonable and adequate data security to protect Plaintiffs and Class members' Private Information, and compensatory damages.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and All Class Members)

310. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

311. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII/PHI; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

312. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

313. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

314. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII/PHI.

315. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

316. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT VI
Breach of Confidence
(On Behalf of Plaintiffs and All Class Members)

317. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

318. Plaintiffs and Class Members have an interest, both equitable and legal, in their Private Information that was conveyed to, collected by, and maintained by Defendant - and that was accessed or compromised in the Data Breach.

319. Defendant was provided with and stored private and valuable PHI related to Plaintiffs and the Class, which it was required to maintain in confidence.

320. Plaintiffs and the Class provided Defendant with their personal and confidential PHI under both the express and/or implied agreement of Defendant to limit the use and disclosure of such PHI.

321. Defendant owed a duty to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

322. Defendant had an obligation to maintain the confidentiality of Plaintiffs and Class Members' PHI.

323. Plaintiffs and Class Members have a privacy interest in their personal medical matters, and Defendant had a duty not to disclose confidential medical information and records concerning its patients.

324. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PHI and confidential medical records of Plaintiffs and Class Members.

325. Plaintiffs' and Class Members' PHI is not generally known to the public and is confidential by nature.

326. Plaintiffs and Class Members did not consent to nor authorize Defendant to release or disclose their PHI to unknown criminal actors.

327. Defendant breached the duties of confidence it owed to Plaintiffs and Class Members when Plaintiffs and Class Members' PHI was disclosed to unknown criminal hackers.

328. Defendant breached its duties of confidence by failing to safeguard Plaintiffs and Class Members' PHI, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and

practices published to its patients; (h) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs and Class Members' PHI and medical records/information to a criminal third party.

329. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiffs and Class Members, their privacy, confidences, and PHI would not have been compromised.

330. As a direct and proximate result of Defendant's breach of Plaintiffs and Class Members' confidences, Plaintiffs and Class Members have suffered injuries, including:

a. Loss of their privacy and confidentiality in their PHI;

b. Theft of their Private Information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

h. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs and Class Members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members' data;

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant; and

k. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

331. Additionally, Defendant received payments from Plaintiffs and Class Members for services with the understanding that Defendant would uphold its responsibilities to maintain the confidences of Plaintiffs and Class Members' private medical information.

332. Defendant breached the confidence of Plaintiffs and Class Members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiffs' and Class Members' expense.

333. As a direct and proximate result of Defendant's breach of its duty of confidences, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
Breach of Bailment
(On Behalf of Plaintiffs and All Class Members)

334. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

335. Plaintiffs and the Class delivered their PII and PHI to Defendant as part of the implicit agreement described above and only for the limited purposes of their employment and/or ambulance services.

336. Defendant was not permitted to use the PHI or PII for its own purposes except to provide services and/or employment to Plaintiffs and the Class.

337. Defendant was expected to delete such data when it was no longer necessary to provide the required services or employment, and Defendant was no longer required to by law to retain such PII and/or PHI.

338. At no point did Plaintiffs or the Class relinquish ownership over their PII and PHI and expected that it would be returned or deleted without disclosure to unauthorized third parties.

339. Defendant breached the bailment agreement by failing to protect the data in accordance with Defendant's legal obligations and thus allowing the data to be disclosure to unauthorized cybercriminals, which subjected Plaintiffs and the Class to the harms outlined above.

340. Defendant must compensate Plaintiffs and the Class for their injuries and must be required to implement cybersecurity safeguards sufficient to guard against further breaches of the bailment Agreement.

341. Alternatively, Defendant must destroy Plaintiffs and the Class Members data if permitted by law.

COUNT VIII
Violation of the Louisiana Unfair Trade Practices & Consumer Protection Law
La. Rev. Stat. §§ 51:1401 *et seq.*
(On behalf of Louisiana Plaintiffs & the Louisiana Class)

342. Louisiana Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

343. The Louisiana Unfair Trade Practices and Consumer Protection Law (the "LUTPA") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

344. Louisiana Plaintiffs, Louisiana Class Members and Defendant are "persons" within the meaning of La. Rev. Stat. Ann. § 51:1402(8).

345. Louisiana Plaintiffs and Louisiana Class Members are "consumers" within the meaning of La. Rev. Stat. § 51:1402(1).

346. Defendant participated in unfair and deceptive practices that violated the LUTPA, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Louisiana Plaintiffs and Louisiana Class Members, which were direct and proximate causes of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which were direct and proximate causes of the Data Breach;

c. Misrepresenting that Defendant would protect the privacy and confidentiality of Louisiana Plaintiffs' and Louisiana Class Members' Private Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Louisiana Plaintiffs' and Louisiana Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45;

e. Omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Louisiana Plaintiffs' and Louisiana Class Members' Private Information; and

f. Omitting, suppressing, and concealing the material fact that Defendant did not comply with its common law and statutory duties pertaining to the security and privacy of Louisiana Plaintiffs' and Louisiana Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45.

347. Defendant intended to mislead the Louisiana Plaintiffs and Louisiana Class Members and induce them to rely on its misrepresentations and omissions.

348. Defendant's unfair and deceptive acts and practices were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Louisiana Plaintiffs and Louisiana Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

349. Defendant acted intentionally, knowingly, and maliciously to violate the LUTPA and recklessly disregarded Louisiana Plaintiffs' and Louisiana Class Members' rights.

350. Had Defendant disclosed to Louisiana Plaintiffs and Louisiana Class Members that its data systems were not secure and thus vulnerable to cyber-attacks, Defendant would have been unable to continue its business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant accepted the role of "steward of the data" while keeping its inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself as having a special role as a healthcare provider with corresponding duty of trustworthiness and care, Louisiana Plaintiffs and Louisiana Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

351. As a direct and proximate result of these unfair and deceptive acts and practices, Louisiana Plaintiffs and each Louisiana Class Member suffered actual harm and will continue to suffer injury, ascertainable losses of money and/or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; increased, imminent risk of fraud and identity theft; and loss of value of the Private Information.

352. Defendant's misrepresentations and omissions were material to consumers and made in order to induce consumers' reliance regarding the safety and security of Private Information in order to obtain consumers' Private Information and purchase of medical products and/or services.

353. Defendant's deceptive practices misled Louisiana Plaintiffs and the Louisiana Class and would cause a reasonable person to enter into transactions with Defendant that resulted in damages.

354. As such, Louisiana Plaintiffs and the Louisiana Class seek all monetary and non-monetary relief allowed by law, including: (1) actual damages sustained; (2) treble damages for Defendant's knowing violations of the LUTPA; (3) reasonable attorneys' fees and costs; (4) declaratory relief and (5) such equity relief as the Court deems necessary or proper to protect Louisiana Plaintiffs and the members of the Louisiana Class from Defendant's deceptive conduct.

COUNT IX
Violation of the Louisiana Database Security Breach Notification Law
La. Rev. Stat. §§ 51:3071 *et seq.*
(On behalf of Louisiana Plaintiffs & the Louisiana Class)

355. Louisiana Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs.

356. Louisiana Plaintiffs, Louisiana Class Members and Defendant are "persons" within the meaning of La. Rev. Stat. § 51:3073(3).

357. The Private Information disclosed in Defendant's Data Breach qualifies as "Personal Information as defined in La. Rev. Stat. § 51:3073(4)(a) because it contains the "first name or first initial and last name of an individual resident in the state in combination with any or more of the following data elements. . . Social Security number."

358. Under La. Rev. Stat. § 51:3074(A), "Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

359. As explained above, Defendant failed to implement reasonable security measures to protect Louisiana Plaintiffs' and Louisiana Class Members' Private Information, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Louisiana Plaintiffs and Louisiana Class Members, which were direct and proximate causes of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which were direct and proximate causes of the Data Breach;

c. Misrepresenting that Defendant would protect the privacy and confidentiality of Louisiana Plaintiffs' and Louisiana Class Members' Private Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Louisiana Plaintiffs' and Louisiana Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45;

e. Omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Louisiana Plaintiffs' and Louisiana Class Members' Private Information; and

f. Omitting, suppressing, and concealing the material fact that Defendant did not comply with its common law and statutory duties pertaining to the security and privacy of Louisiana Plaintiffs' and Louisiana Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45.

360. A violation of the La. Rev. Stat. § 51:3074(A) shall be considered "an unfair act or practice pursuant to R.S. 51:1405(A)."

361. Defendant's unfair and deceptive acts or practices were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Louisiana Plaintiffs and Louisiana Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

362. Defendant acted intentionally, knowingly, and maliciously to violate the LUTPA and recklessly disregarded Louisiana Plaintiffs' and Louisiana Class Members' rights. Had Defendant disclosed to Louisiana Plaintiffs and Louisiana Class Members that its data systems were not secure and thus vulnerable to cyber-attacks, Defendant would have been unable to continue its business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant accepted the role of "steward of the data" while keeping its inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself as having a special role as a healthcare provider with corresponding duty of trustworthiness and care, Louisiana Plaintiffs and Louisiana Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

363. As a direct and proximate result of these unfair and deceptive acts and practices, Louisiana Plaintiffs and each Louisiana Class Member suffered actual harm and will continue to suffer injury, ascertainable losses of money and/or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; increased, imminent risk of fraud and identity theft; and loss of value of the Private Information.

364. Defendant's misrepresentations and omissions were material to consumers and made in order to induce consumers' reliance regarding the safety and security of Private Information in order to obtain consumers' Private Information and purchase of medical products and/or services.

365. Defendant's deceptive practices misled Louisiana Plaintiffs and the Louisiana Class and would cause a reasonable person to enter into transactions with Defendant that resulted in damages.

366. As such, Louisiana Plaintiffs and the Louisiana Class seek all monetary and non-monetary relief allowed by law, including: (1) actual damages sustained; (2) treble damages for Defendant's knowing violations of the LUTPA; (3) reasonable attorneys' fees and costs; (4) declaratory relief and (5) such equity relief as the Court deems necessary or proper to protect Louisiana Plaintiffs and the members of the Louisiana Class from Defendant's deceptive conduct.

COUNT X
Declaratory Judgment and Equitable Relief.
(On behalf of Plaintiffs & all Class Members)

367. Plaintiffs re-allege and incorporate by reference all the allegations contained in the preceding paragraphs. Plaintiffs brings this claim individually and on behalf of the Class.

368. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

369. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Defendant is currently maintaining data

security measures adequate to protect Plaintiffs' and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and PHI will occur in the future.

370. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

371. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

372. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant's properties.

373. The risk of another such breach is real, immediate and substantial.

374. If another breach of Defendant's store of patient data occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

375. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft

and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

376. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant [what], thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the Defendant and that the Court grant the following:

A. For an Order certifying the Classes and appointing Plaintiffs and Counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII and PHI, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant network is compromised, hackers cannot gain access to other portions of Defendant systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and

assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: November 22, 2024

Respectfully Submitted,

/s/ Andrew A. Lemmon

Andrew A. Lemmon (LA Bar No. 18302)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5301 Canal Boulevard, Suite A
New Orleans, Louisiana 70124
Tel.: (985)783-6789
Email: alemmon@milberg.com

Gary M. Klinger (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878
Email: gklinger@milberg.com

Jeff Ostrow (*pro hac vice*)
KOPELOWIT ZOSTROW FERGUSON WEISELBERG GILBERT
1 West Las Olas, Suite 500
Fort Lauderdale, Florida 33301
T: (954) 525-4100 / F: (954) 525-4300
ostrow@kolawyers.com

Terence R. Coates (*pro hac vice*)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 665-0204
Email: tcoates@msdlegal.com

Plaintiffs' Interim Co-Lead Counsel

CERTIFICATE OF SERVICE

I certify that on the 22nd day of November 2024, the foregoing document was filed electronically with the Clerk of Court using the Court's CM/ECF system. Notice of this filing will be sent to counsel for all parties by operation of the CM/ECF system.

/s/ *Andrew A. Lemmon*
Andrew A. Lemmon